PATENT ABSTRACTS OF JAPAN

(11)Publication number : 60-203036
(43)Date of publication of application : 14.10.1985

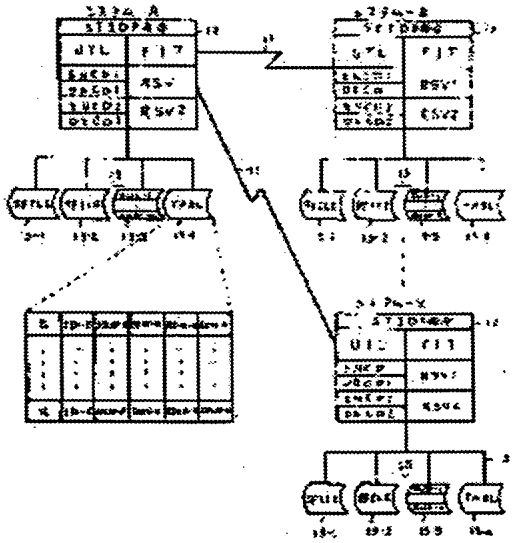
(51)Int.Cl. H04L 9/00
G09C 1/00

(21)Application number : 59-058245
(22)Date of filing : 28.03.1984

(71)Applicant : HITACHI LTD
(72)Inventor : MATSUKI TAKESHI

(54) PRIVACY COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To prevent the wiretap by providing a means which selects and registers the individual coding and decoding procedures through mutual communication for each remote side of communication.
CONSTITUTION: When a system A has the privacy communication with a system B, both the name B and identification number ID-B of the system are supplied to a utility program UTL for privacy communication. The program UTL uses a coding subroutine ENCD1 to perform the coding procedure and carries out a wiring action to a control table 13-4 for privacy communication in a direct access memory 13 of the system A. Thus the system A completes the registration of the system B for communication. In the same way, the system B registers the system A of the remote side. Hereafter, the privacy communication system can be freely set and changed by means of the program UTL.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭60－203036

⑤Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和60年(1985)10月14日
H 04 L 9/00		Z－7240－5K	
G 09 C 1/00		7368－5B	

審査請求　未請求　発明の数 1　（全5頁）

⑭発明の名称　秘密通信方式

⑳特　願　昭59－58245
㉒出　願　昭59(1984)3月28日

㉗発明者　松木　武　横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内
㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉔代理人　弁理士　高橋　明夫　外1名

明　細　書

1．発明の名称

秘密通信方式

2．特許請求の範囲

(1) 複数の装置間で相互に通信を行う通信ネットワーク・システムにおいて、該システム構成要素の各装置に、複数種類の暗号化、復号化操作手順を内蔵すると共に通信相手ごとの暗号化、復号化操作手順を相互の通信によって選択する手段を設け、前記選択された暗号化、復号化操作手順により通信相手ごとに個別に暗号化、復号化を行うことを特徴とする秘密通信方式。

3．発明の詳細な説明

〔発明の利用分野〕

本発明は、複数の装置間で相互に通信を行うネットワーク・システムにおける秘密通信方式に関する。

〔発明の背景〕

従来の秘密通信の多くは、規格化された暗号化方式(DES：Data Encryption Standard)にもとづいている。ところが、DESは暗号化鍵と復号化鍵が同一でなければならないため、相互に秘密通信を行なう装置が複雑に絡み合っている多数存在するネットワークでは、暗号鍵の秘密を守ることは困難であった。

一方、このDESの欠点を補う方法として公開鍵暗号法がある。この公開鍵による暗号化と秘密鍵による復号化を別々の鍵を用いて行うことにより、鍵配送に限れば、問題はなくなったと云える。しかしながら、複雑なネットワークの中で秘密通信を行うためには、鍵配送の問題以前に、秘密通信の方式の取り決めを当事者以外が漏れないようにいかに行うかの問題がある。複雑なネットワークでは、秘密通信の送信者、受信者の関係は交錯しているため、秘密通信の方式を、1対の送信者と受信者のあいだで秘密に取り決めようとしても、他の通信相手にも内容が漏れてしまう恐れが強く、機密保持が難かしい。

〔発明の目的〕

本発明は、上述した欠点を解消するためになさ

れたもので、複数の装置間の秘密通信において、1対の秘密通信の当事者間における処理方式や暗号鍵などの機密事項が他者に漏洩するのを防ぎ、信頼性の高い秘密通信方式を提供することを目的とする。

〔発明の概要〕

本発明は複数の装置間で相互に通信を行うネットワーク・システムにおいて、ネットワーク構成要素の各装置に、複数種の暗号化、復号化操作手順を内蔵すると共に、通信相手ごとの暗号化、復号化操作手順を相互の通信によって選択し登録する手段を設けることによって、通信相手ごとに個別の暗号化、復号化操作を行うことを特徴とするものである。

〔発明の実施例〕

第1図は本発明の一実施例を示すシステム構成図である。第1図において、複数のシステム（装置）A，B，…，Xが通信回線11で結ばれており、それぞれのシステムは中央処理装置12（以下CPUと略す）と直接アクセス記憶装置13（以下DASDと略す）を具備している。各CPU12には個別の識別番号（以下CPUIDと略す）が割り当てられている。CPU12の主記憶装置には、ファイル伝送プログラムFITと秘密通信用ユティリティプログラムUTL、UTL用の暗号化サブルーチンENCD1とENCD2、UTL用の復号化サブルーチンDECD1とDECD2が格納されるとともに、FIT用の暗号化復号化サブルーチンSUB－1，…，SUB－nをDASD13中のライブラリ13－3から実行時に動的にローディングするためのエリアRSV1とRSV2が含まれる。DASD13には、FIT用の送信ファイル（SFILE）13－1、同受信ファイル（RFILE）13－2、暗号化復号化サブルーチンSUB－1，…，SUB－nを格納したライブラリ13－3と、秘密通信管理用テーブルのファイル（TABL）13－4が含まれる。TABL13－4は、通信相手のシステムの名称（例えばB）、CPUID（例えばID－B）、FITで送信時に使用する暗号化サブルーチンの名称（例えばSSUB－B）と暗号化鍵（例えばSKEY－B）、FITで受信時に使用する復号化サブルーチンの名称（例えばRSUB－B）と復号化鍵（例えばRKEY－B）から構成される。

次にシステムーAとシステムーBが秘密通信を行う場合を例に、その処理手順を説明する。

第2図は、システムーAに通信相手（システムーB）を登録する手順を示すフローチャートである。まず、通信相手のシステムの名称（B）とCPUID（ID－B）をシステムーAの秘密通信用ユティリティプログラムUTLに与える（ステップ201）。UTLでは、与えられたシステム名称BとCPU識別番号ID－Bの値を暗号化サブルーチンENCD1を用いて暗号化する（ステップ202）。暗号化したBとID－BをシステムーAのDASD13中のTABL13－4に書き込む（ステップ203）。これで、システムーAでの通信相手システムーBの登録が終わる。同様にシステムーBで通信相手システムーAを登録することより、以後、UTLプログラムを用いて自由に秘密通信の方式を設定、変更できる。

本実施例では、秘密通信の方式の設定、変更は、受信側のシステムが主導権を持って行うとする。第3図はシステムーAがシステムーBから秘密通信を受信する場合の、秘密通信方式の設定と変更の処理手順を示すフローチャートである。まず、システムーAの秘密通信用ユティリティプログラムUTLに、システムーAがシステムーBから受信する場合の暗号化、復号化操作手順名と、暗号化鍵、復号化鍵を生成する元になる乱数を与える（ステップ301）。次に、暗号化、復号化操作手順名から、システムーBがシステムーAに送信するときにシステムーBで使用する暗号化サブルーチン名SSUB－Aと、システムーAがシステムーBから受信したときにシステムーAで使用する復号化サブルーチン名RSUB－Bを求める（ステップ302）。さらに乱数から、暗号化、復号化操作手順に合致した暗号化鍵SKEY－Aと復号化鍵RKEY－Bを生成する（ステップ3

０３）。次に、第４図で詳述する手順で、ＣＰＵＩＤのやりとりをシステムーＡとシステムーＢの間で行うことにより、通信相手の正当性を確認する（ステップ３０４，３０５）。通信相手が不当の場合は異常終了となるが、正当の場合は、暗号化鍵ＳＫＥＹーＡと暗号化サブルーチン名ＳＳＵＢーＡを暗号化サブルーチンＥＮＣＤ２で暗号化したのち、システムーＢのＵＴＬに送信する（ステップ３０６，３０７）。システムーＢのＵＴＬでは、受信したＳＫＥＹーＡとＳＳＵＢーＡを復号化サブルーチンＤＥＣＯ２で復号化したのち、再度暗号化サブルーチンＥＮＣＤＩで暗号化し、システムーＢのＤＡＳＤ１３中のＴＡＢＬ１３ー４に書き込む（ステップ３０８，３０９，３１０）。システムーＡのＵＴＬは、復号化鍵ＲＫＥＹーＢと復号化サブルーチン名ＲＳＵＢーＢを暗号化サブルーチンＥＮＣＤＩで暗号化したのち、システムーＡのＴＡＢＬ１３ー４に書き込む（ステップ３１１，３１２）。

以上でシステムーＡがシステムーＢから受信する場合の秘密通信方式の設定、変更を終了するが、同様の操作をシステムーＢが主体となって行うことにより、システムーＢがシステムーＡから受信する場合の秘密通信方式の設定、変更が遂成される。この双方での秘密通信方式の設定、変更を終了することで、システムーＡとシステムーＢの間の秘密通信の送受信が可能となる。

第４図は通信相手の確認を行うときの処理手順を示したフローチャートである。まず、システムーＡのＵＴＬは、ＳＴＩＤＰ命令でＣＰＵＩＤ（ＩＤーＡ）を求める（ステップ４０１）。システム名ＡとＣＰＵＩＤ（ＩＤーＡ）を暗号化サブルーチンＥＮＣＤ２で暗号化したのち、システムーＢのＵＴＬに送信する（ステップ４０２，４０３）。システムーＢのＵＴＬは受信したシステム名ＡとＣＰＵＩＤ（ＩＤーＡ）を復号化サブルーチンＤＥＣＤ２で復号化し（ステップ４０４）、システムーＢのＴＡＢＬ１３ー４から読み込んで復号化サブルーチンＤＥＣＤＩで復号化したシステム名およびＣＰＵＩＤと比較する（ステップ４０５，４０６）。このとき、ＴＡＢＬ１３ー４中にシステム名Ａが登録されて無かったり、ＣＰＵＩＤが不一致の場合は、不当な通信相手とみなして異常終了する。ＣＰＵＩＤが一致した場合は、同様の手順を逆方向に行って相互に通信相手の正当性を確認する（ステップ４０７～４１２）。

第５図は実際に秘密通信を行う場合の手順を示すフローチャートで、システムーＢからシステムーＡにファイルを送信する場合の例を示したものである。まず、前述の第４図の手順で通信相手の確認を行い（ステップ５０１）、不当な通信相手の場合は異常終了する。通信相手が正当の場合は、システムーＢで次の処理を行って暗号化操作手順を準備する。まず、システムーＢのＴＡＢＬ１３ー４からシステムーＡに送信する場合の暗号化鍵ＳＫＥＹーＡと暗号化サブルーチン名ＳＳＵＢーＡを読み込み、復号化サブルーチンＤＥＣＤＩで復号化する（ステップ５０２，５０３）。次に、ＳＳＵＢーＡに対応する暗号化サブルーチンＳＵＢーｉをＤＡＳＤ１３中のライブラリ１３ー３からシステムーＢの主記憶装置中のＲＳＶＩエリアにローディングする（ステップ５０４）。他方、システムーＡでは次の処理を行って復号化操作手順を準備する。まず、システムーＡのＴＡＢＬ１３ー４からシステムーＢから受信する場合の復号化鍵ＲＫＥＹーＢと復号化サブルーチン名ＲＳＵＢーＢを読み込み、復号化サブルーチンＤＥＣＤＩで復号化する（ステップ５０５，５０６）。次に、ＲＳＵＢーＢに対応する復号化サブルーチンＳＵＢーｊをＤＡＳＤ１３中のライブラリ１３ー３からシステムーＡの主記憶装置中のＲＳＶ２エリアにローディングする（ステップ５０７）。これで暗号化、復号化操作手順が準備できたことになる。

次にシステムーＢは送信ファイル（ＳＦＩＬＥ）１３ー１から１レコード入力し、暗号化鍵ＳＫＥＹーＡと暗号化サブルーチンＳＵＢーｊで該レコードを暗号化して、システムーＡにＦＩＴプログラムを用いて送信する（ステップ５０８，５０９，５１０）。システムーＡでは受信したレコードを

復号化鍵ＲＫＥＹ－Ｂと復号化サブルーチンＳＵＢ－ｊで復号化したのち、システムーＡの受信ファイル（ＲＦＩＬＥ）１３－２に書き込む（ステップ５１１，５１２）。以下ステップ５０８から５１２までの処理をシステムーＢの送信ファイル（ＳＦＩＬＥ）１３－１の最終レコードまで繰り返し、秘密通信によるファイル伝送を終了する（ステップ５１３）。

なお、本実施例において、ＥＮＣＤ１とＤＥＣＤ１のサブルーチンを用いて、ＤＡＳＤ１３中のＴＡＢＬファイル１３－４を暗号化復号化しているのは、不当なユーザがＴＡＢＬファイルを参照して、機密を知ることができないようにするためであり、また、通信相手の確認時にＥＮＣＤ２とＤＥＣＤ２のサブルーチンを用いてメッセージを暗号化復号化しているのも、同様な理由からである。

以上、実施例に於いてはファイル伝送での秘密通信について説明したが、本発明はこれに限らず、一般のオンラインコントロールプログラムに適用することにより、複数システムのオンラインコントロールプログラム間の通信内容の盗聴を確実に防止することができ、システムの機密保護機能の信頼性が向上される。

〔発明の効果〕

本発明によれば、事前に通信相手システムや装置を相互に登録しておくだけで、暗号化、復号化操作手順や暗号鍵を秘密通信の一方の当事者が、自由に設定あるいは変更できるようになり、複雑なネットワークにおいても、通信相手ごとに個別の暗号化、復号化操作手順や暗号鍵を秘密に設定することができる。したがって、万が一、通信内容が正当な通信相手以外に漏れても、その内容を解読することは困難であり、複数システムや装置を含むネットワークにおいて、信頼度の高い秘密通信を行うことができる。

3．発明の詳細な説明

第１図は本発明の一実施例のシステム構成図、第２図は通信相手を登録する処理フロー図、第３図は秘密通信方式の設定と変更の処理フロー図、第４図は通信相手の確認を行う処理フロー図、第５図は実際に秘密通信を行う場合の処理フロー図である。

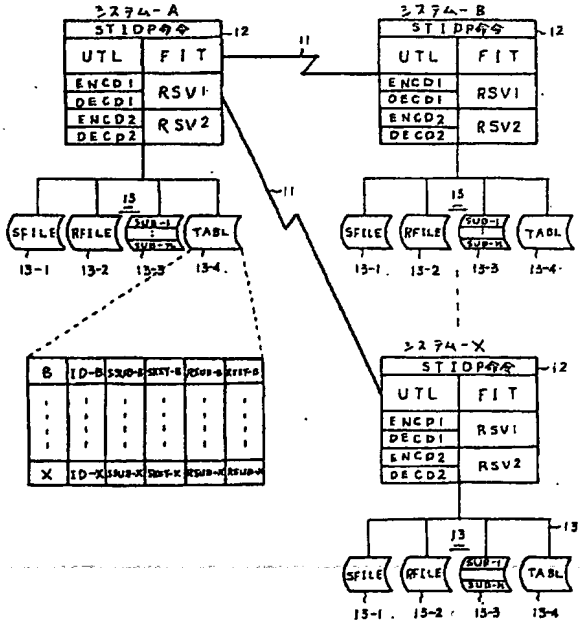
１１…通信回線、　１２…中央処理装置、

１３－１…送信ファイル、　１３－２…受信ファイル、　１３－３…暗号化復号化サブルーチン、

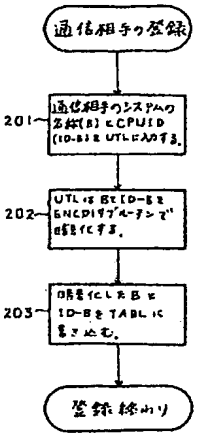
１３－４…秘密通信管理用テーブル、　ＦＩＴ…ファイル伝送プログラム、　ＵＴＬ…秘密通信用ユティリティプログラム。

代理人弁理士　高　橋　明

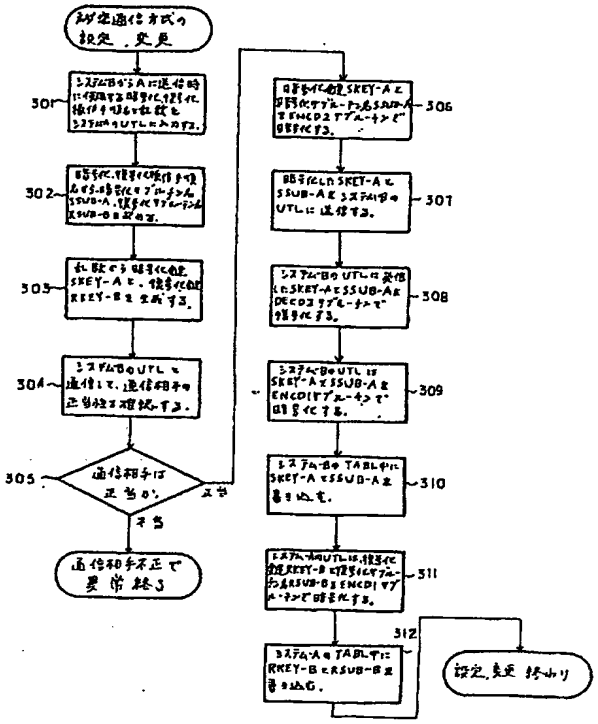
第 1 図



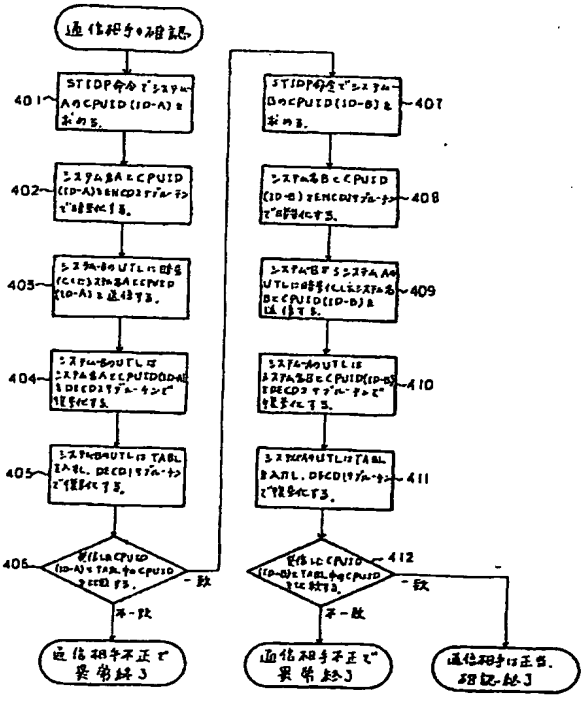
第 2 図



第 3 図



第 4 図



第 5 図